January 31, 2024

Dear Members of the Committee:

Public Citizen submits this testimony in support of H.B. 697.

On behalf of our 16,859 members and activists in the Commonwealth of Virginia, and more than 500,000 supporters nationwide, Public Citizen encourages the Committee on Courts of Justice to advance H.B. 697, a legislative proposal to address the dangers of deceptive and fraudulent computer-generated deepfakes.

Extraordinary advances in the realm of Artificial Intelligence (A.I.) now provide any person with the means to produce computer-generated fake images, audio or videos of individuals doing or saying things that they never actually did or said. This fabricated content, also known as "deepfakes" can be used to fraudulently misrepresent the actions of another person.

Deepfake technology is rapidly improving. In August of this past year the NIH put out a study that found that 27-50% of ppl cannot identify deepfake videos. Technologists have said that soon, even they will not be able to tell what is real content versus a deepfake.
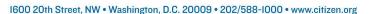
In the hands of bad actors - this technology can be used in a myriad of ways to cause significant harm.

Two of the many realms in which we are already seeing deepfakes being used to cause harm are in regards to non-consensual sexual images and political communications.

Sexual deepfakes are fabricated images and videos that depict individuals naked and/or performing a sexual acts. Hundreds of thousands of these have been created and uploaded to the internet without the victim's consent. The vast majority of those targeted are women, and children are frequently being targeted as well.

Recently, sexual deepfakes of Taylor Swift were circulated widely which led to a public outcry. However, this is happening frequently to everyday people. Take, for example. 14 year old Francesca Mani who learned that boys at her highschool had circulated sexual deepfakes of her and 30 other girls.

Deepfake technology also has some particularly alarming implications as we approach the upcoming elections. The use of deepfakes in elections communications can be very dangerous, as we have already witnessed in other countries. Two days before Slovakia's elections, a

fraudulent audio deepfake was disseminated on social media of the leader of the Progressive Slovakia party purportedly discussing ways to rig the election. It is believed that this deepfake influenced the outcome of the Slovakian election. We also saw rampant use of deepfakes in recent major elections in Argentina and Turkey as well.

We are starting to see the use of political deepfakes ramp up in the U.S. as we approach the 2024 elections, Recently, in an attempt to disrupt the Presidential Primary Election, voters in New Hampshire received a robocall from an AI generated deepfake of President Joe Biden's voice.

The rapid development of deepfake technology also threatens to further weaken social trust in our society. As deepfakes become more common, it will become more difficult for people to determine what is real and what is fabricated content. Additionally, it will become easier for bad actors to refute real visual or audio evidence of their bad behavior, by claiming it is a deepfake. All of this will serve to undermine public trust in news and information.

Deepfakes pose very real and present threats to our society. We must have common sense safeguards in place to prevent abuse of this technology bad actors. New legislation, like H.B. 697, is needed to regulate the use of deepfakes in our society.

Public Citizen strongly urges the Committee on Courts of Justice to move H.B. 697 forward as an important step towards putting critical protections in place to protect Virginians from the harms of deepfakes.

Respectfully Submitted,
Ilana Beller
Public Citizen